

**CASIG 5 – Operaciones de Ciberseguridad**

**Preguntas de Auditoría**

**Controlar los Cambios de Configuración**

**Competencias Básicas del Auditor**

**1. Conocimiento en Sistemas de Información y Arquitecturas de TI:** Un auditor debe comprender cómo funcionan los sistemas de información, incluyendo hardware, software, redes y bases de datos. Debe estar familiarizado con las arquitecturas de TI más comunes y cómo se interconectan sus componentes.

**2.Entendimiento de Estándares y Marcos de Ciberseguridad:** Es esencial que el auditor conozca y comprenda los estándares y marcos de referencia en ciberseguridad, como ISO 27001, NIST SP 800-53 y CIS Controls. Estos proporcionan las mejores prácticas y directrices para la gestión de la configuración y otros aspectos de la ciberseguridad.

**3.Habilidades en Herramientas de Auditoría y Análisis:** El auditor debe ser competente en el uso de herramientas específicas de auditoría que permitan evaluar y analizar configuraciones, detectar vulnerabilidades y validar la conformidad con las políticas y estándares establecidos.

**4.Conocimiento en Gestión de Cambios y Control de Versiones:** Dado que la gestión de la configuración implica cambios constantes, el auditor debe entender cómo se gestionan, aprueban y documentan estos cambios. Además, debe conocer sistemas de control de versiones para rastrear y validar las modificaciones en los CIs.

**5.Competencia en Evaluación de Riesgos y Análisis de Impacto:** El auditor debe ser capaz de identificar y evaluar riesgos asociados con configuraciones inadecuadas o no autorizadas. Además, debe poder determinar el impacto potencial de cualquier desviación o vulnerabilidad en la seguridad y operatividad del sistema.

# Visión General

Este control ayuda a mantener la seguridad, privacidad y funcionalidad adecuada del sistema, evitando cambios no autorizados que puedan comprometer la integridad de los activos de TI. A través de un proceso formal de revisión y autorización de cambios, la organización garantiza que todos los ajustes realizados en la configuración de los sistemas cumplan con los requisitos organizacionales y regulatorios.

**1.1 Proceso de Revisión y Autorización de Cambios**  
Cada cambio en el sistema debe pasar por un proceso de revisión exhaustivo en el cual se evalúan los impactos en la seguridad y la privacidad antes de la aprobación. Los cambios propuestos se documentan y se notifican a las partes interesadas relevantes, quienes pueden aprobar o desaprobar las modificaciones con base en un análisis de impacto detallado. Este proceso incluye mantener registros completos de todos los cambios autorizados y desautorizar cualquier modificación que no cuente con la aprobación formal. Después de que se implementa un cambio, es importante verificar que los controles de seguridad y privacidad afectados se hayan aplicado correctamente y que estos estén cumpliendo con los requisitos esperados. Asimismo, se establecen restricciones de acceso físico y lógico para los cambios, limitando los privilegios de quienes pueden modificar los componentes del sistema y asegurando que se aplique la autorización dual en el proceso.

**1.2 Auditoría y Monitoreo de Cambios en Configuración**  
Desde la perspectiva de auditoría, es esencial monitorear continuamente los cambios controlados por la configuración para asegurar que cada modificación se realice conforme a los procedimientos de gestión de cambios. La auditoría se centra en revisar que solo los cambios autorizados se implementen y en evaluar la precisión de los registros asociados. Indicadores específicos, como el número de cambios no autorizados y el porcentaje de precisión en los cambios de estado en comparación con la línea base de configuración, ayudan a medir el rendimiento de la actividad de control de cambios. Además, la auditoría verifica que los representantes de seguridad y privacidad formen parte del comité de aprobación de cambios y que los cambios se prueben, validen y documenten adecuadamente antes de su implementación final. Este monitoreo continuo y la implementación de mecanismos automatizados para mantener la línea base de configuración contribuyen a garantizar la integridad, precisión y disponibilidad de los sistemas, fortaleciendo así el entorno operativo.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Determinar y documentar los tipos de cambios en el sistema que están controlados por la gestión de configuración 2. Revisar los cambios propuestos controlados por la configuración en el sistema y aprobar o desaprobar dichos cambios con consideración explícita para los análisis de impacto de seguridad y privacidad 3. Conservar registros de cambios controlados por la configuración en el sistema. 4. Notificar a las partes interesadas correspondientes sobre los cambios propuestos en el sistema. Solicitar la aprobación de cambios cuando corresponda. 5. Después de los cambios en el sistema, verifique que los controles afectados se implementen correctamente, funcionen según lo previsto y produzcan el resultado deseado con respecto al cumplimiento de los requisitos de seguridad y privacidad del sistema. 6. Definir, documentar, aprobar y aplicar restricciones de acceso físico y lógico asociadas con cambios en el sistema. Aplicar la autorización dual para implementar cambios 7. Limitar los privilegios para cambiar los componentes del sistema y la información relacionada con el sistema dentro de un entorno operativo o de producción 8. Configurar el sistema para proporcionar sólo funcionalidad mínima |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Documentar las decisiones de cambio de configuración asociadas con el sistema 2. Probar, validar y documentar los cambios en el sistema antes de finalizar la implementación del cambio 3. Requerir que representantes de seguridad y privacidad sean miembros del comité de aprobación de cambios. 4. Destacar los cambios propuestos al sistema que no hayan sido aprobados o desaprobado dentro de un período de tiempo definido por la organización. 5. Prohibir los cambios introducidos en el sistema hasta que se reciban las aprobaciones designadas. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Establecer indicadores cuantitativos específicos para la medición del desempeño y rendimiento de esta actividad, tales como: 2. Número de cambios no autorizados identificados 3. Porcentaje de precisión en los cambios de estado de los CIs en comparación con las líneas de referencia |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Supervisar y revisar las actividades asociadas con los cambios controlados por la configuración en el sistema 2. Analizar los cambios en el sistema para determinar los posibles impactos en la seguridad y la privacidad antes de la implementación del cambio |
| NIVEL 5 [Optimizado]: La organización se centra en la mejora continua y está diseñada para girar y responder a las oportunidades y los cambios. | 1. Mantener la vigencia, integridad, precisión y disponibilidad de la línea base de configuración de los sistemas utilizando mecanismos automatizados. |

1. **Preguntas de Auditoría para Controlar los Cambios de Configuración**

|  |
| --- |
| * 1. **Temática: Control de Cambios de Configuración** |
| En esta evaluación, los auditores deben centrarse en examinar cómo la organización implementa y supervisa los procedimientos de gestión de cambios. Esto incluye la revisión de las políticas de control de cambios para asegurarse de que son adecuadas, la verificación de que existan procesos claramente definidos para la solicitud, revisión, aprobación e implementación de cambios, y la comprobación de la existencia de registros detallados de todos los cambios realizados.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización determina los tipos de cambios en el sistema que requieren control de configuración?   + Revisar la política o protocolo de gestión de configuración para identificar criterios o directrices sobre qué cambios requieren control.   + ¿Dónde y cómo se documentan estos tipos de cambios controlados?     - Solicitar y revisar la documentación que lista y describe los tipos de cambios controlados. Asegurarse de que esté actualizada y sea accesible para las partes relevantes. * ¿Se revisa y actualiza periódicamente la lista de tipos de cambios controlados?   + Revisar registros de revisiones anteriores y entrevistar al equipo de gestión de configuraciones para entender la frecuencia y el proceso de revisión. * ¿Existen mecanismos para adaptar y expandir los tipos de cambios controlados basados en la evolución del sistema o las necesidades del negocio? * ¿La organización realiza el análisis de impacto de seguridad y privacidad para los cambios propuestos?   + Solicitar y revisar ejemplos de análisis de impacto realizados para cambios anteriores. * ¿Se ha establecido un responsable de aprobar o desaprobar los cambios propuestos? * ¿Se mantiene un registro de las decisiones tomadas sobre los cambios propuestos?   + Solicitar registros de decisiones de cambios anteriores y validar que se documenten adecuadamente las justificaciones y consideraciones. * ¿Qué criterios se utilizan para aprobar o desaprobar un cambio propuesto?   + Revisar la política o protocolo de aprobación de cambios y validar que se consideren aspectos de seguridad y privacidad. * ¿Cómo se asegura que los cambios no aprobados no se implementen en el sistema?   + Revisar los mecanismos de control y monitoreo post-decisión.   + Entrevistar al equipo de operaciones para entender cómo se gestionan los cambios no aprobados. * ¿Cómo se verifica la correcta implementación de los controles afectados después de un cambio?   + Solicitar y revisar procedimientos post-cambio y registros de verificación. Considerar realizar pruebas spot para validar la implementación de controles. * ¿Existen pruebas automatizadas o manuales para asegurar que los controles funcionen según lo previsto? * ¿Cómo se valida que los controles cumplen con los requisitos de seguridad y privacidad después de un cambio?   + Solicitar evidencia de revisiones de cumplimiento post-cambio y entrevistar al equipo de seguridad para entender el proceso de validación. * ¿Qué acciones se toman si se identifica que un control no funciona como se esperaba después de un cambio?   + Revisar protocolos de respuesta a fallos en controles y solicitar ejemplos de acciones tomadas en situaciones anteriores. |

|  |
| --- |
| * 1. **Temática: Registro de los Cambios Controlados** |
| El registro adecuado de los cambios controlados proporciona una trazabilidad completa de todas las modificaciones realizadas en los sistemas, aplicaciones y redes de una organización. Este registro detallado incluye información sobre la naturaleza del cambio, quién lo autorizó, quién lo implementó, cuándo se realizó y qué resultados se obtuvieron. La documentación exhaustiva de los cambios controlados asegura que cualquier modificación en el entorno de TI pueda ser revisada y evaluada en términos de impacto, efectividad y seguridad, contribuyendo significativamente a la integridad y estabilidad de los sistemas de información de la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Dónde y cómo se conservan los registros de cambios controlados?   + Solicitar y revisar ejemplos de registros de cambios. Asegurarse de que estén organizados, sean accesibles y estén protegidos adecuadamente.   + ¿Durante cuánto tiempo se conservan estos registros?     - ¿Cumple con la política de retención de registros? * ¿Qué información se incluye en los registros de cambios, contienen detalles suficientes sobre el cambio, la justificación, la aprobación y cualquier impacto asociado? * ¿Cómo se asegura la integridad y autenticidad de los registros de cambios?   + Revisar los mecanismos de protección y control de acceso a los registros. Considerar la posibilidad de entrevistar al equipo de seguridad para entender las medidas de protección. * ¿Cómo se gestiona y responde a la retroalimentación o preocupaciones de las partes interesadas sobre los cambios propuestos? |

|  |
| --- |
| * 1. **Temática: Controles Básicos sobre los Cambios** |
| La implementación de controles básicos sobre los cambios en la configuración de los sistemas incluye procedimientos para la solicitud, revisión, aprobación y documentación de todos los cambios, así como la evaluación de su impacto antes de la implementación. Los controles básicos también abarcan la necesidad de comunicar los cambios a todas las partes interesadas relevantes y la realización de pruebas post-implementación para asegurar que los cambios funcionen como se esperaba sin introducir nuevos problemas o vulnerabilidades.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cómo se definen y documentan las restricciones de acceso relacionadas con los cambios en el sistema?   + Solicite y revise la documentación que define las restricciones de acceso. * ¿Qué mecanismos se utilizan para aplicar la autorización dual en la implementación de cambios?   + Revisar herramientas o sistemas que requieran múltiples autorizaciones y solicitar registros de cambios anteriores que demuestren la autorización dual. * ¿Cómo se asegura que las restricciones de acceso se aplican correctamente después de un cambio?   + Realizar pruebas spot o solicitar evidencia de pruebas que validen las restricciones de acceso post-cambio. * ¿Cómo se determinan y asignan los privilegios para realizar cambios en el sistema?   + Solicitar y revisar la política de asignación de privilegios y entrevistar al equipo de gestión de accesos. * ¿Existen controles para prevenir cambios no autorizados en el entorno de producción? * ¿Cómo se auditan y registran los cambios realizados en el entorno de producción?   + ¿Qué acciones se toman si se detecta un cambio no autorizado en el entorno de producción?     - Revisar protocolos de respuesta a incidentes y solicitar ejemplos de acciones tomadas en situaciones anteriores. * ¿Cómo se revisan y actualizan periódicamente los privilegios de acceso al entorno de producción? * ¿Cómo se determina la funcionalidad mínima necesaria para el sistema?   + Revisar la documentación de diseño y arquitectura del sistema y entrevistar a las partes interesadas para entender las necesidades funcionales. * ¿Qué mecanismos se utilizan para asegurar que el sistema esté configurado con funcionalidad mínima? |

|  |
| --- |
| * 1. **Temática: Comunicación a las partes interesadas** |
| La comunicación efectiva a las partes interesadas implica informar de manera oportuna y precisa a todos los individuos y departamentos relevantes sobre los cambios planificados, sus potenciales impactos, el cronograma de implementación y cualquier acción requerida por su parte. Esta transparencia fomenta la colaboración, reduce la resistencia al cambio y minimiza el riesgo de interrupciones inesperadas en los servicios. Además, asegura que las partes interesadas estén preparadas para adaptarse a los nuevos entornos o procesos y puedan contribuir de manera proactiva a la detección y resolución de posibles problemas que surjan como resultado de los cambios.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cómo se identifican las partes interesadas que deben ser notificadas sobre los cambios propuestos?   + Revisar la política o protocolo de comunicación de cambios y validar que se identifiquen adecuadamente las partes interesadas. * ¿Qué mecanismos se utilizan para notificar a las partes interesadas sobre los cambios propuestos?   + Solicitar ejemplos de comunicaciones recientes y revisar los canales de comunicación utilizados. * ¿Cómo se solicita y registra la aprobación de las partes interesadas para los cambios propuestos? * ¿Qué criterios se utilizan para determinar cuándo es necesario solicitar la aprobación de las partes interesadas?   + Revisar la política o protocolo de aprobación y validar que se consideren las necesidades y responsabilidades de las partes interesadas. |